GlobalResearch
Center for Research on Globalization

Wikileaks Reveals: CIA's UMBRAGE Allows Agency to Carry out 'False Flag' Cyber Attacks

By Whitney Webb
Global Research, April 15, 2019
Mint Press News 7 March 2017

Region: USA
Theme: Intelligence

This Mint Press article was first posted on Global Research on March 10, 2017

A new release of CIA documents by Wikileaks indicates that the intelligence agency has the means and the intent to mask the cyber-attacks it commits by making them seem as if they originated from a foreign power.

Earlier today, Wikileaks once again made headlines following its release of the "largest ever publication of U.S. Central Intelligence Agency (CIA) documents." The massive release – just the first batch in a trove of documents code-named "Vault 7" by Wikileaks – details the CIA's global covert hacking program and its arsenal of weaponized exploits.

While most coverage thus far has focused on the CIA's ability to infiltrate and hack smartphones, smart TVs and several encrypted messaging applications, another crucial aspect of this latest leak has been skimmed over – one with potentially far-reaching geopolitical implications.

According to a Wikileaks press release, the 8,761 newly published files came from the CIA's Center for Cyber Intelligence (CCI) in Langley, Virginia. The release says that the UMBRAGE group, a subdivision of the center's Remote Development Branch (RDB), has been collecting and maintaining a "substantial library of attack techniques 'stolen' from malware produced in other states, including the Russian Federation."

As Wikileaks notes, the UMBRAGE group and its related projects allow the CIA to misdirect the attribution of cyber attacks by "leaving behind the 'fingerprints' of the very groups that the attack techniques were stolen from."

In other words, the CIA's sophisticated hacking tools all have a "signature" marking them as originating from the agency. In order to avoid arousing suspicion as to the true extent of its covert cyber operations, the CIA has employed UMBRAGE's techniques in order to create signatures that allow multiple attacks to be attributed to various entities – instead of the real point of origin at the CIA – while also increasing its total number of attack types.

Other parts of the release similarly focus on avoiding the attribution of cyberattacks or malware infestations to the CIA during forensic reviews of such attacks. In a document titled "Development Tradecraft DOs and DON'Ts," hackers and code writers are warned "DO NOT leave data in a binary file that demonstrates CIA, U.S. [government] or its witting partner companies' involvement in the creation or use of the binary/tool." It then states that "attribution of binary/tool/etc. by an adversary can cause irreversible impacts to past,

present and future U.S. [government] operations and equities."

While a major motivating factor in the CIA's use of UMBRAGE is to cover its tracks, events over the past few months suggest that UMBRAGE may have been used for other, more nefarious purposes. After the outcome of the 2016 U.S. presidential election shocked many within the U.S. political establishment and corporate-owned media, the CIA emerged claiming that Russia mounted a "covert intelligence operation" to help Donald Trump edge out his rival Hillary Clinton.

Prior to the election, Clinton's campaign had also accused Russia of being behind the leak of John Podesta's emails, as well as the emails of employees of the Democratic National Committee (DNC).

Last December, Director of National Intelligence James Clapper – a man known for lying under oath about NSA surveillance – briefed senators in a closed-door meeting where he described findings on Russian government "hacks and other interference" in the election.

Following the meeting, Rep. Adam Schiff (D-CA), a ranking member of the House Intelligence Committee,remarked: "After many briefings by our intelligence community, it is clear to me that the Russians hacked our democratic institutions and sought to interfere in our elections and sow discord."

Incidentally, the U.S. intelligence community's assertions that Russia used cyber-attacks to interfere with the election overshadowed reports that the U.S. government had actually been responsible for several hacking attempts that targeted state election systems. For instance, the state of Georgia reported numerous hacking attempts on its election agencies' networks, nearly all of which were traced back to the U.S. Department of Homeland Security.

Now that the CIA has been shown to not only have the capability but also the express intention of replacing the "fingerprint" of cyber-attacks it conducts with those of another state actor, the CIA's alleged evidence that Russia hacked the U.S. election – or anything else for that matter – is immediately suspect. There is no longer any way to determine if the CIA's proof of Russian hacks on U.S. infrastructure is legitimate, as it could very well be a "false flag" attack.

Given that accusations of Russian government cyber-attacks also coincide with a historic low in diplomatic relations between Russia and the U.S., the CIA's long history of using covert means to justify hostile actions against foreign powers – typically in the name of national security – once again seems to be in play.

Whitney Webb is a MintPress contributor who has written for several news organizations in both English and Spanish; her stories have been featured on ZeroHedge, the Anti-Media, 21st Century Wire, and True Activist among others – she currently resides in Southern Chile.

Become a Member of Global Research

Articles by: Whitney Webb